AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, at ~~the intermediate device~~ a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information;

receiving, at ~~the intermediate device~~ a DHCP relay agent process of the router, from the host, a ~~first~~ DHCP discovery message for discovering a logical network address for the host;

generating at the DHCP relay agent process a second message based on the ~~first~~ DHCP discovery message and the first data; and

sending the second message from the DHCP relay agent process to a ~~second~~ DHCP server that provides the logical network address for the host;

wherein ~~an authenticator process performs said step of receiving the first data; a relay agent process for the second server performs said steps of receiving the first message and sending the second message; the relay agent process is separate from the authenticator process; and~~ generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data.

2. (Canceled)

3. (Previously presented) A method as recited in Claim 1, wherein:

the step of generating the second message further comprises the steps of:

storing second data based on the first data by the authenticator process; and

retrieving the second data by the relay agent process in response to said step of receiving the first message.

4. (Original) A method as recited in Claim 1, wherein the first server is an authentication, authorization and accounting server.

5. (Original) A method as recited in Claim 4, wherein the first server is a RADIUS protocol server.

6. (Currently amended) A method as recited in Claim 1, wherein the physical connection comprises an Ethernet interface card on the ~~intermediate device~~router.

7. (Original) A method as recited in Claim 1, wherein the physical connection comprises a wireless Ethernet encryption key and time slot.

8. (Original) A method as recited in Claim 1, wherein the request for authentication is based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

9. (Canceled)

10. (Original) A method as recited in Claim 1, wherein:
the first data includes user class data indicating a particular group of one or more authorized users of the host; and
said step of generating the second message is further based on the user class data.

11. (Original) A method as recited in Claim 1, wherein:
the first data includes credential data indicating authentication is performed by the first server; and
said step of generating the second message is further based on the credential data.

12.-25. (Canceled)

26. (Currently amended) An apparatus for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, comprising:

means for receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information;

means for receiving, at a DHCP relay agent process of the router, from the host, a ~~first~~ DHCP discovery message for discovering a logical network address for the host;

means for generating at the DHCP relay agent process a second message based on the ~~first~~ DHCP discovery message and the first data; and

means for sending the second message from the DHCP relay agent process to a ~~second~~ DHCP server that provides the logical network address for the host;

wherein ~~an authenticator process performs said step of receiving the first data; a relay agent process for the second server performs said steps of receiving the first message and sending the second message; the relay agent process is separate from the authenticator process; and~~ generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data.

27. (Currently amended) An apparatus for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a physical connection that is coupled to the host;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving, at an authenticator process for the host, through the network interface from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information;

receiving, at a DHCP relay agent process, through the physical connection from the host, a ~~first~~ DHCP discovery message for discovering a logical network address for the host;

generating at the DHCP relay agent process a second message based on the ~~first~~ DHCP discovery message and the first data; and

sending through the network interface the second message from the DHCP relay agent process to a ~~second~~ DHCP server that provides the logical network address for the host;

wherein ~~an authenticator process performs said step of receiving the first data; a relay agent process for the second server performs said steps of receiving the first message and sending the second message; the relay agent process is separate from the authenticator process; and~~ generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data.

28. (New) A computer-readable medium carrying one or more sequences of instructions for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information;

receiving, at a DHCP relay agent process of the router, from the host, a DHCP discovery message for discovering a logical network address for the host;

generating at the DHCP relay agent process a second message based on the DHCP discovery message and the first data; and

sending the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host;

wherein generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data.

29. (New) An apparatus as recited in Claim 26, wherein the means for generating the second message further comprises means for storing second data based on the first data by the authenticator process, and means for retrieving the second data by the relay agent process in response to said step of receiving the first message.

30. (New) An apparatus as recited in Claim 26, wherein the physical connection comprises any one of an Ethernet interface card, and a wireless Ethernet encryption key and time slot.

31. (New) An apparatus as recited in Claim 26, wherein the request for authentication is based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

32. (New) An apparatus as recited in Claim 26, wherein the first data includes user class data indicating a particular group of one or more authorized users of the host; and wherein the means for generating the second message comprises means for generating the second message based on the user class data.

33. (New) An apparatus as recited in Claim 26, wherein the first data includes credential data indicating authentication is performed by the first server; and wherein the means for generating the second message further comprises means for generating the second message based on the credential data.

34. (New) An apparatus as recited in Claim 27, wherein the instructions for generating the second message further comprise instructions for storing second data based on the first data by the authenticator process, and instructions for retrieving the second data by the relay agent process in response to receiving the first message.

35. (New) An apparatus as recited in Claim 27, wherein the physical connection comprises any one of an Ethernet interface card, and a wireless Ethernet encryption key and time slot.

36. (New) An apparatus as recited in Claim 27, wherein the request for authentication is based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

37. (New) An apparatus as recited in Claim 27, wherein the first data includes user class data indicating a particular group of one or more authorized users of the host; and wherein the instructions for generating the second message comprise further instructions for generating the second message based on the user class data.

38. (New) An apparatus as recited in Claim 27, wherein the first data includes credential data indicating authentication is performed by the first server; and wherein the instructions for

generating the second message further comprise instructions for generating the second message based on the credential data.